


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)
Search: ☒ The ACM Digital Library ☐ The Guide



Searching within **The ACM Digital Library** for: elliptic curve binary series hidden point ([start a new search](#))
 Found **16** of **264,269**

REFINE YOUR SEARCH
[Search Results](#)
[Related Journals](#)
[Related Magazines](#)
[Related SI](#)

 Sort by [relevance](#)

Results 1 - 16 of 16

▼ **Refine by Keywords**

[Discover Terms](#)

▼ **Refine by People**

[Names](#)
[Institutions](#)
[Authors](#)
[Editors](#)
[Reviewers](#)

▼ **Refine by Publications**

[Publication Year](#)
[Publication Names](#)
[ACM Publications](#)
[All Publications](#)
[Content Formats](#)
[Publishers](#)

▼ **Refine by Conferences**

[Sponsors](#)
[Events](#)
[Proceeding Series](#)

[Save results to a Binder](#)

1 [Communications of the ACM: Volume 51 Issue 1](#)

 January 2008 [Communications of the ACM](#)
Publisher: ACM

 Full text available: [Digital Edition](#) , [Pdf \(5.97 MB\)](#) Additional Information: [full citation](#)
Bibliometrics: Downloads (6 Weeks): 673, Downloads (12 Months): 3166, Downloads (All Time): 10000

2 [Side-channel resistant system-level design flow for public-key cryptography](#)

Kazuo Sakiyama, Eike De Mulder, Bart Preneel, Ingrid Verbauwhede

 March 2007 **GLSVLSI '07: Proceedings of the 17th ACM Great Lakes symposium on VLSI**
Publisher: ACM [Request Permissions](#)

 Full text available: [Pdf \(650.57 KB\)](#) Additional Information: [full citation](#), [abstract](#)
Bibliometrics: Downloads (6 Weeks): 7, Downloads (12 Months): 42, Downloads (All Time): 100

In this paper, we propose a new design methodology to assess the risk of side-channel attacks. The methodology consists of a timing analysis and simple power analysis, at an early design stage. This methodology is applied to a side-channel resistant elliptic curve cryptographic hardware design.

Keywords: elliptic curve cryptography, side-channel attack, system-level design

3 [Reconfigurable computing: a survey of systems and software](#)

Katherine Compton, Scott Hauck

 June 2002 **Computing Surveys (CSUR)** , Volume 34 Issue 2

Publisher: ACM [Request Permissions](#)

 Full text available: [Pdf \(710.56 KB\)](#) Additional Information: [full citation](#), [abstract](#)
Bibliometrics: Downloads (6 Weeks): 122, Downloads (12 Months): 883, Downloads (All Time): 1000

Due to its potential to greatly accelerate a wide variety of applications, reconfigurable computing has become a subject of a great deal of research. Its key feature is the ability to perform a wide variety of functions, while retaining the performance of dedicated hardware.

Keywords: Automatic design, FPGA, field-programmable gate array, manual design, reconfigurable computing, reconfigurable systems

4 [A survey of RFID privacy approaches](#)

Marc Langheinrich

 August 2009 **Personal and Ubiquitous Computing** , Volume 13 Issue 6

Publisher: Springer-Verlag



ADVANCED SEARCH
[Advanced Search](#)
FEEDBACK

Please provide us with feedback



 Found **16** of **264,269**

Full text available:  Pdf (308.39 KB)Additional Information: [full citation](#), [abstract](#)**Bibliometrics:** Downloads (6 Weeks): 220, Downloads (12 Months): 350, Downloads (24 Months): 450


A bewildering number of proposals have offered solutions to the privacy problem. This article tries to give an overview of the currently discussed approaches.

Keywords: Privacy, RFID**5** [On the power of simple branch prediction analysis](#) [Onur Adigmez, Cetin Kaya Koc, Jean-Pierre Seifert](#)March 2007 **ASIACCS '07: Proceedings of the 2nd ACM symposium on Information security****Publisher:** ACM  [Request Permissions](#)Full text available:  Pdf (3.40 MB)Additional Information: [full citation](#), [abstract](#)**Bibliometrics:** Downloads (6 Weeks): 16, Downloads (12 Months): 95, Downloads (24 Months): 120

Very recently, a new software side-channel attack, called Branch Prediction Analysis, was discovered and also demonstrated to be practically feasible on popular processors. The recent attack still had the flavor of a classic timing attack.




Keywords: RSA, branch prediction analysis, modular exponentiation, side-channel attack**6** [MAX: Wide area human-centric search of the physical world](#) [Kok-KI ONG Yap, Vikram Srinivasan, Mehul Motani](#)August 2008 **Transactions on Sensor Networks (TOSN)**, Volume 4 Issue 4**Publisher:** ACM  [Request Permissions](#)Full text available:  Pdf (6.03 MB)Additional Information: [full citation](#), [abstract](#)**Bibliometrics:** Downloads (6 Weeks): 22, Downloads (12 Months): 203, Downloads (24 Months): 250

We propose MAX, a system that facilitates human-centric search of the physical world. a priori, it allows humans to search for and locate them as needed. Designing a human-centric operation, ...




Keywords: Human-centric, landmark-based localization, physical world**7** [Proceedings of the 2005 ACM symposium on Applied computing](#) [Hisham M. Haddad, Andrea Omicini, Roger L. Wainwright, Lorie M. Liebrock](#)March 2005 **SAC '05: Proceedings of the 2005 ACM symposium on Applied computing****Publisher:** ACMAdditional Information: [full citation](#), [abstract](#)**Bibliometrics:** Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (24 Months): n/a

Welcome to the 20th Annual ACM Symposium on Applied Computing (SAC) on Mining and Technology, Socorro, New Mexico, USA. As the Conference organizing committee, thank you for participating ...




8 [Level set and PDE methods for computer graphics](#)

-  [David Breen, Ron Fedkiw, Ken Museth, Stanley Osher, Guillermo Sapiro, R...](#)
August 2004 **SIGGRAPH '04: SIGGRAPH 2004 Course Notes**
Publisher: ACM  [Request Permissions](#)
Full text available:  Pdf (17.07 MB) Additional Information: [full citation](#), [abstract](#)
Bibliometrics: Downloads (6 Weeks): 131, Downloads (12 Months): 1050, Downloads (All Time): 1050




Level set methods, an important class of partial differential equation (PDE) implicitly as the level set (iso-surface) of a sampled, evolving nD function. This material introduces the ...

- 9** [The elements of nature: interactive and realistic techniques](#)
 [Oliver Deussen, David S. Eberl, Ron Fedkiw, E. Kenton Musgrave, Przemyslaw Tessendorf](#)
August 2004 **SIGGRAPH '04: SIGGRAPH 2004 Course Notes**
Publisher: ACM  [Request Permissions](#)
Full text available:  Pdf (17.65 MB) Additional Information: [full citation](#), [abstract](#)
Bibliometrics: Downloads (6 Weeks): 220, Downloads (12 Months): 1551, Downloads (All Time): 1551

This updated course on simulating natural phenomena will cover the latest in simulating most of the elements of nature. The presenters will provide research perspectives ...

- 10** [GPGPU: general purpose computation on graphics hardware](#)
 [David Luebke, Mark Harris, Jens Krüger, Tim Purcell, Naga Govindaraju, Ja...](#)
August 2004 **SIGGRAPH '04: SIGGRAPH 2004 Course Notes**
Publisher: ACM  [Request Permissions](#)
Full text available:  Pdf (63.03 MB) Additional Information: [full citation](#), [abstract](#)
Bibliometrics: Downloads (6 Weeks): 244, Downloads (12 Months): 1625, Downloads (All Time): 1625




The graphics processor (GPU) on today's commodity video cards has evolved into a general purpose processor. The latest graphics architectures provide tremendous memory bandwidth with fully programmable vertex ...

- 11** [Design, implementation and testing of extended and mixed precision BLAS](#)
 [Xiaoye S. Li, James W. Demmel, David H. Bailey, Greg Henry, Yozo Hida, J...](#)
June 2002 **Transactions on Mathematical Software (TOMS)**, Volume 28, Number 2
Publisher: ACM  [Request Permissions](#)
Full text available:  Pdf (456.84 KB) Additional Information: [full citation](#), [abstract](#)
Bibliometrics: Downloads (6 Weeks): 10, Downloads (12 Months): 87, Downloads (All Time): 87

This article describes the design rationale, a C implementation, and conformance testing of the BLAS (Basic Linear Algebra Subroutines): Extended and Mixed Precision BLAS ...

Keywords: BLAS, double-double arithmetic, extended and mixed precision




- 12** [A review of vessel extraction techniques and algorithms](#)
[Cemil Kirbas, Francis Quek](#)

- June 2004 **Computing Surveys (CSUR)**, Volume 36 Issue 2
 **Publisher:** ACM  [Request Permissions](#)
 Full text available:  Pdf (8.06 MB) Additional Information: [full citation](#), [abstract](#)
Bibliometrics: Downloads (6 Weeks): 89, Downloads (12 Months): 699, Download

Vessel segmentation algorithms are the critical components of circulator
 a survey of vessel extraction techniques and algorithms. We put the var
 techniques in perspective ...

Keywords: Magnetic resonance angiography, X-ray angiography, medi




13 [The data mining approach to automated software testing](#)

-  [Mark Last](#), [Menahem Friedman](#), [Abraham Kandel](#)
 August 2003 **KDD '03**: Proceedings of the ninth ACM SIGKDD internationa
 mining
Publisher: ACM  [Request Permissions](#)
 Full text available:  Pdf (296.40 KB) Additional Information: [full citation](#), [abstract](#)
Bibliometrics: Downloads (6 Weeks): 53, Downloads (12 Months): 338, Downl

In today's industry, the design of software tests is mostly based on the
 are limited to execution of pre-planned tests only. Evaluation of test out
 effort by human ...

Keywords: automated software testing, finite element solver, info-fuzz
 testing




14 [A system for understanding imaged infographics and its applications](#)

-  [Wei-hua Huang](#), [Chew Lim Tan](#)
 August 2007 **DocEng '07**: Proceedings of the 2007 ACM symposium on Doc
Publisher: ACM  [Request Permissions](#)
 Full text available:  Pdf (1.13 MB) Additional Information: [full citation](#), [abstract](#)
Bibliometrics: Downloads (6 Weeks): 14, Downloads (12 Months): 59, Downlo

Information graphics, or infographics, are visual representations of infor
 infographics in documents is a relatively new research problem, which b
 appear as raster images. ...

Keywords: applications, association of text and graphics, document im

15 [Artistic screening](#)


-  [Victor Ostromoukhov](#), [Roger D. Hersch](#)
 September 1995 **SIGGRAPH '95**: Proceedings of the 22nd annual conferen
 techniques
Publisher: ACM  [Request Permissions](#)
 Full text available:  Pdf (4.15 MB) Additional Information: [full citation](#), [reference](#)
Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 44, Downloa

Keywords: artistic screening, graphic design, halftoning, image reprod

16 [Shrouds: optimal separating surfaces for enumerated volumes](#)

Gregory M. Nielson, Gary Grai, Ryan Holmes, Adam Huang, Mariano Phielig
May 2003 **VISSYM '03: Proceedings of the symposium on Data visualis**

Publisher: Eurographics Association

Full text available:  [Pdf](#) (1.58 MB)

Additional Information: [full citation](#), [abst](#)

Bibliometrics: Downloads (6 Weeks): 1, Downloads (12 Months): 8, Download

We describe new techniques for computing a smooth triangular mesh su
consisting of a collection of points from a 3D rectilinear grid. The surfac
by a marching cubes ...

The ACM Portal is published by the Association for Computing Machinery. Copyright ©

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)